Department of Transportation
Office of Inspector General (OIG)
Status Report of Laptop Investigation
August 22, 2006

Update on Notifying Affected Individuals:

Working from a backup file, we want to personally notify each individual whose information may have been contained in the databases stored on the laptop stolen in Miami. As of close of business August 21, 2006, we have mailed approximately 62,000 letters and are working to obtain addresses for the remaining individuals so we can complete the mailing as quickly as possible.

In Addition, We are Focusing on Four Major Priorities:

1. Recovery of the laptop stolen in Miami. We currently have 12 agents on the ground working with the Miami-Dade County police, who are providing valuable assistance in our attempt to recover this laptop, which was password protected in accordance with National Institute of Standards and Technology protocols. We are actively pursuing several leads, including some reported to OIG's hotline (800-424-9071; staffed 24 hours a day, seven days a week). We have also established a $10,000 reward for information leading to the recovery of the laptop and/or arrest of the perpetrator(s).

2. Fully, thoroughly, and expeditiously completing our investigation into the facts and circumstances surrounding the theft of the Miami laptop. The Acting Inspector General immediately ordered this investigation upon learning that the stolen laptop contained personally-identifiable information

(PII). He also directed that the investigation be expanded to take another look at the theft of a second laptop issued to a senior investigator also assigned to the Miami office. That theft occurred on April 24, 2006, from a hotel meeting room at a conference in Orlando. These were the first laptops reported missing by our investigators since they began using laptops over 10 years ago.

3. Determining what Departmental and OIG policies relating to the protection of sensitive information and computer security were applicable to these thefts, including reporting requirements, *and* whether these policies were followed in both cases.

4. Strengthening policies and procedures so OIG keeps its commitment that such a breach will never happen again and, in the process, serves as a model in government for safeguarding PII and other sensitive information. As part of this effort, we are reviewing options for obtaining the assistance of an outside expert in computer security and privacy requirements to identify additional actions we can take to enhance our internal controls.

   The Acting Inspector General has already issued several directives related to these priorities, including:

   - All OIG investigators have been instructed not to leave government laptops or electronic storage media unattended in vehicles, even if the vehicle is locked. Current policy requires investigators to immediately report the loss or theft of any computer or other electronic media storage device to their supervisor and the OIG information systems security officer. In the event of a theft, investigators are required to report it immediately to the local law enforcement authority and submit a copy of the police report to Headquarters within 48 hours.

   - All OIG employees were instructed to remove any databases containing PII from laptops and to ensure that all sensitive data is stored in encrypted folders. Each OIG employee has been directed to certify compliance with this requirement and OIG managers were instructed to verify employees' compliance.

   - All OIG employees have been directed to re-certify by August 28, 2006, that they have read and understood Departmental guidance on safeguarding information and computer security.

- All OIG employees have been told to complete the Department's new Privacy Act and updated computer security awareness training by August 30, 2006.

- We are developing PII policies that will be consistent with soon-to-be-announced DOT policies being established pursuant to the Office of Management and Budget's July 12, 2006, memorandum directing Chief Information Officers to strengthen controls over PII data.

- On August 14, 2006, the Acting IG held an all-OIG employee web cast to reinforce requirements for safeguarding sensitive information on computer hardware and storage media.

Other Ongoing Significant Activities:

- Fully addressing the issues raised by 16 Members of the Florida congressional delegation in their letter of August 11, 2006. We understand and appreciate the concerns expressed by Members of the Florida congressional delegation over this incident. We will respond promptly to their letter, and when we complete our analysis we will provide a detailed description of our current procedures and protocols for handling this type of PII information and steps we are taking to ensure that a loss like this does not occur again.

- Personally notifying each individual whose information was contained in databases stored on the Miami laptop. We are contacting those persons whose data was contained on the backup file for the laptop stolen in Miami. As of close of business August 21, 2006, we have mailed approximately 62,000 letters and are working to obtain addresses for the remaining individuals so we can complete the mailing as quickly as possible.

  We are recommending that affected individuals: contact one of the three major credit reporting bureaus to request that an initial fraud alert be placed on their credit record (which entitles them to one free credit report form each company); monitor bank and credit card statements and contact financial institutions to check for any suspicious activity on their accounts, and; be vigilant to any phone calls, e-mails, and other communications from individuals purporting to be government officials and "phishing" for or asking to verify personal information.

  We are encouraging anyone who suspects they may be a victim of identity theft due to the loss of this laptop to contact our hotline (1-800-

424-9071), staffed 24 hours a day, seven days a week. As of noon today, we have received 427 telephone calls and 19 emails to our hotline from individuals with questions, requests for information, and tips for investigative follow-up.

- Obtaining information on credit protection. We are working with the General Services Administration and Department of Veterans Affairs to obtain information on options for protecting the credit of those individuals whose personal information was contained on the backup file of the stolen Miami laptop.

- Completing forensic analysis of material stored on both the stolen Miami and Orlando laptops. We are continuing to analyze backups of these laptop hard drives to fully identify what type of information and documents may have been stored on the laptops. Should we find any additional databases containing PII material, we will make further notifications, as appropriate.

Other Investigative Actions Being Taken:

- We placed one quarter-page advertisements in the Sunday editions of The Miami Herald and El Nuevo Herald announcing our $10,000 reward for information leading to the recovery of the Miami laptop and/or arrest of the perpetrator(s).

- We have handed out over 2,700 fliers announcing our reward to police stations, pawnshops, and used-computer stores in the Miami area (to view our reward poster, please go to our special site on the web at: http://www.oig.dot.gov/rewardposter_eng.pdf).

- We are also collaborating with Crime Stoppers of Miami-Dade, which has offered an additional $1,000 award for information about the stolen laptop.

- OIG investigators and local police have visited more than 350 pawnshops in the Miami-Dade County area and inspected laptops that were for sale.

- OIG investigators and the Miami-Dade County police have conducted more than 800 field interviews. The FBI is also providing assistance.

- During the past two weekends, OIG investigators and local police have made 21 visits to flea markets in the Miami-Dade County area looking for the stolen laptop and distributing fliers.

- We have reviewed the recovered-stolen property inventories from eight local police agencies and the Florida Highway Patrol.